International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.2, No.10, October 2013 DOI:10.15693/ijaist/2013.v2i10.27-32

Monitoring Tools For Network Services And System

Sujindar.S[#1], Malini.K [#2], Rakesh.S[*3]

[#] Department of Computer Science and Engineering, Adithya Institute of Technology,

*Assistant Professor , Department of Computer Science, Adithya Institute of Technology, Kurumbapalayam, Coimbatore, India

***Abstract*—Network monitoring tools are used to monitor the system for problems caused by overloaded or crashed servers. There are various network monitoring tools for managing systems or software's today. This paper analyses few Network Monitoring tools on comparative study of features, performance, and security for managing and securing systems or software's.**

Keyword-Monitoring, Wireless, Security, Performance, OpenSource

I. INTRODUCTION

Network Monitoring have become more and more important. In earlier days, Network administrators, might only monitor a fewer Network devices. More sophisticated monitoring systems are needed in order to maintain network stability. Network monitoring tools constantly monitors a computer network and notifies the system administrators in case any failures. Different Notification methods used are E-mail, land-line and cell Phones, SMS, fax, etc. This paper provide a detailed view on each tool on different category such as wireless networks, Data Collection, Log Collection, Monitoring services or servers, and information Security. We have discussed the features, performance, and security of each tool so that the user can select the tool according to their requirements.

II. DIFFERENT MONITORING TOOLS

A. *AirWave:*

Airwave is a powerful and user friendly product developed by Aruba Networks to manage WLAN and remote access solutions [1]. AirWave allows managing several generations of multivendor networks. Unlike traditional port-based management, Airwave employs a user-centric approach, identifying who is on the network, where they are accessing the network , the mobile devices they are using , how much bandwidth is being consumed by specific devices. AirWave gives the clarity and control needed to effectively manage enterprise mobility , providing real time monitoring , proactive alerts , historical reporting and fast , efficient troubleshooting through a user Interface. AirWave provides a clear and accurate picture of who is on the network, their location and how the devices in the network are performing. AirWave identifies the most relevant threats and greatly reduces the false-positives that improve the network security [2]. Airwave reduces cost and complexity, improves service quality, and helps IT make intelligent.

Features:

1) Fault Management
   - Alarm Filtering
   - Alarm Generation
   - Clear Correlation
   - Fault Detection
   - SNMP 'Trapping'

2) Configuration Management
   - Auto Discovery
   - Configuration Templates
   - Copy configuration
   - Real time Change Notifications
   - Scheduled Configuration Change

3) Performance Management
   - Availability Monitoring
   - Conditional Alerts
   - Hardware Monitoring
   - Performance Report generation
   - Traffic Analysis
   - Wireless Network Management

B. *Cisco WCS (Wireless control system)*

Cisco Wireless Control System helps to successfully plan, deploy, monitor, troubleshoot, and report on indoor and outdoor wireless networks. WCS delivers high-performance applications and mission critical solutions that improve productivity. It gives a platform for small, midsize, large-scale wireless LANs across local, remote, national and international locations. WCS help to efficiently implement and maintain secure wireless LANs, all from a centralize locations[3]. WCS, User friendly GUI reduces operational costs, improves efficiency in a large network. It operates as a single unified platform, incorporating the full breadth of management requirements, from radio frequency to controllers to services.

WCS provides platform for monitoring entire wireless LAN to maintain high performance and deliver optimal wireless experience to mobile users. WCS alarm simplifies access to critical information and faults which facilitates faster assessment of notifications.

Advantages:

1. Graphs, Charts and tables are interactive for quicker configuration and re-configuration.
2. Hierarchical mapping trees, color coding and icons support quick visualization and status assessments of network, devices, and air quality.
3. Alarm Management.

C. 7Signal Sapphire

7Signal sapphire [4] is specifically designed to enable businesses to meet the challenges of today's wireless networking requirements and SLA's. Sapphire resolves issues of Connectivity, Latency, Packet loss, Delays, Throughput, Voice quality, Success rates and Interference points[5]. Sapphire allows to measure end-to-end connection quality for all clients on the network. Sapphire is fully automated, fast to deploy solution which provides quality monitoring, reporting of alarms and proactive fault prevention for any vendor's wireless network[6]. Sapphire is only performance solution that pinpoints performance issues before users or administrators are aware of the issues. Three main elements which assist sapphire to measure, record, report, alarm, analyse, troubleshoot and verify WLANs

1. *Sapphire Sonar Server:*
   Sonar test servers are located in close proximity to application servers. Sonar Server is the endpoint for user experience measurement performed by the Eye units. Sonar reports results back to Eye units and then forwards those reports to Carat Management Server.

2. *Sapphire Carat Management Server:*
   A centrally located Carat server stores, manages and analyses the collected data from Eyes. It provides reports and alarms.

3. *Sapphire Eye:*
   A simple ceiling-mounted device that measure large wireless Coverage areas.

Features:

- Automated, 24/7 performance monitoring, reporting and alarming.
- Network log change functionality and tracking of performance impacts Client view, true end-to-end, covering LAN/WAN network connections
- Deep remote troubleshooting capabilities
- Perfect companion for Cisco WSC/NCS and Aruba Airwave systems
- WLAN network vendor agnostic, neutral assessment of performance and quality
- Fast and easy to deploy, and no software needed at client terminals
- Software runs on virtual servers; scalable and cost efficient

Advantages:

1. Improved throughput and reduced outages.
2. Avoid unnecessary investments.
3. Cap network management costs.
4. Meet compliance and reporting responsibilities.

D. Big Sister

Big Sister [7] is a real time system and network health monitoring application. Big sister System is licensed under the GNU General Public License is open source software. Big Sister comes in two parts, Status Collector and Agent (uxmon). Agent checks the local status of the local system, network status of neighbouring machines and reports the status periodically to the Status Collector. The Status Collector saves the reported stats, creates webpage showing them, generates alarm messages on pre-configured status changes, collects, stores and displays trend data. Big Sister stores the gathered data in MySQL database or as a plain text files. Big Sister monitors networked systems, provides real time view of current network status, notifies when the system becomes critical, display a variety of system performance data and generates a history of status changes and logs [8]. Big System was originally "Big system network monitor". Now, multiple projects in the realm of system management and monitoring run under the label Big sister. Big Sister intended to be compatible with Big Brother.

E. Cacti

Cacti are open-source, network graphic solution designed as the front-end application to harness the power of RRDTool. Cacti [9] are based on LAMP stack and RRD (Round Robin Database). Cacti are used to monitor network traffic by polling a network switch or router interface by SNMP (Simple network management protocol). Cacti provide faster polls, advanced graph template, multiple data acquisition methods, and user management features. Cacti store all the necessary information in a MySQL database and Round Robin Databases [10]. The frontend of Cacti is completely PHP driven. It can handle multiple users, each with their own graph sets. Cacti handles data gathering and data sources are created corresponding to gathered data. Cacti require a web server, a database, PHP and RDTOOL to configure and work [11] .

Features:

1. Unlimited number of graph items can be defined for each graph.
2. Supports all RRDTool's graph item types.
3. Supports RRD files with more than one data sources.
4. Built in SNMP support that can use php-snmp, ucd-snmp and net-snmp.

5. User based management allows administrators to create users and assign different level of permissions.

F. Cricket

Cricket is a high performance, flexible system designed as a real-time data collection and trending tool, developed to help network managers visualize and understand traffic on their networks. It has two components, a collector and a grapher [12]. The collector runs from "cron" every 5 minutes and stores data into a datastructure managed by RRD Tool. Data are visualized later in graphs through a web-based interface. Cricket uses a hierarchical configuration system called config tree which helps to manage large number of device by specifying the types of data to be collected, how to collect and from where to collect. The config tree is designed to minimize redundant information making it compact, easy to manage and preventing silly mistakes [13]. But the configuration structure of Cricket is bit rigid that makes the debugging of configuration error more difficult. Also one main disadvantage of Cricket is that real-time alerts are extended functionality and not a part of core design. This alert mechanism is called monitor threshold.

G. MRTG

Multi Router Traffic Grapher (MRTG) [14] is open source software that monitors SNMP network devices and provides visual representation of traffic. MRTG reads the traffic counters of routers, logs the data and creates graph representing the monitored network connection. MRTG keeps log of all the data it has pulled from the router and consolidate it so that it does not grow over time. MRTG uses flat file format to store the time related database. MRTG can monitor any SNMP variable [15]. But, In MRTG there is no instance mapping feature. Also in each graph only two counter types can be monitored, in general incoming and outgoing counters.

Features

1. Collects data every five minutes
2. Creates html page per target that features four graphs.
3. Can also send warning email if targets have values above certain threshold.

H. RRDTOOL

RRDtool is the OpenSource high performance data logging and graphing system for time series data. The data's are stored in a round-robin database at a constant interval [16]. The data analysis of RRDtool is based on the ability to quickly generate graphical representation of data value collected over period of time. RRDtool allow updating log file anytime and automatically interpolating any submitted data to fit its internal time-steps. RRDtool offers a special feature data consolidation. After the data is consolidated, the consolidated data point (CDP) is stored in round-robin archive. A round-robin archive stores a fixed number of CDP's and specifies number of primary data points should be consolidated in one CDP and which Consolidated Function (CF) to use. RRDtool supports UNKNOWN value in database, when no new data is available. RRDtool allows generating reports in numerical and graphical form based on the data stored in RRD. The graphing feature is fully configurable. Many tools use RRDtool as a DBMS or graphing subsystem [17].

I. Kiwi syslog

Kiwi syslog [18] collects syslog messages that are sent to it and takes whatever action is defined in the configuration. It is most trusted and offers solution for receiving ,logging ,displaying ,alerting and forwarding syslog, SNMP trap and windows event log messages from devices such as routers, switches, Linux and Unix host, Windows server, etc. Kiwi syslog can be deployed quickly as it accepts syslog [19], SNMP & Event log data from existing deployment. Kiwi syslog displays log locally or anywhere through secure web access module. Kiwi syslog can send email, run programs, or forward data when selected messages arrive. Centralized logs from systems and network devices are used to troubleshoot problems [20].

Features

1. Filtered messages and create advanced alerts.
2. Advanced forwarding options.
3. Converts windows event logs into syslog messages
4. Automatically perform actions based on alerts
5. Trend analysis graphs and email syslog traffic statistics
6. Receive messages via UDP, TCP, SNMP and forward messages.

J. Splunk

Splunk is a fully featured, powerful platform for collecting, searching, and monitoring and analysing machine data. Splunk [21] reads data from source, such as file or port, on a host, classifies that source into sourcetype, then extracts timestamps, breaks up the source into individual events, and writes each event into an index on disk, for lateral retrieval with a search. Splunk monitors and analyses machine data, generated by websites, applications, servers, networks, mobile devices, everything from customer clickstream and transactions to network activity to call records, Splunk turns all the data into valuable insights. It captures indexes and correlates real-time data in a searchable repository from which it can generate graphs, reports, alerts, dashboards and visualizations [22]. When search begins, matching indexed event is retrieved from disk, fields are extracted from the event's text and event is classified by matching against event type.

Features:

1. Monitor systems and infrastructure in real time to identify issues before they impact the systems.

2. Troubleshoot problems and investigate security incidents in minutes.
3. Monitor's end-to-end infrastructure to avoid service degradation or outages.
4. Gain's real-time visibility and critical insights into customer experience, transactions and other key business metrics.
5. Makes the data accessible, valuable and usable.

K. Nagios

Nagios is an open-Source computer system monitoring, network monitoring, and infrastructure monitoring software application [23]. It offers monitoring and alerting services for servers, switches, applications, and services. Nagios are configured to monitor components including system metrics, network protocols, applications, services, servers, and network infrastructure, etc. Nagios alert when these components fail or recover, providing important events. These alerts are received through Email, SMS, or custom scripts. Nagios generate report containing details of outages, events, notifications and alert response [24]. Nagios also offers a web-interface for viewing current network status, notifications, problem history, log files, etc. Multiple users can access the web interface. Nagios stores the data's in text files. But Nagios are quite complex to maintain and use. It does not generate any graphs or statistics. Nagios can be integrated with third-party applications with multiple APIs. Hundreds of community-developed add-ons extend core Nagios functionality [25].

L. RANCID

RANCID (Really Awesome New Cisco config Differ)[26] monitors a router's or devices' configuration, including software and hardware. It uses CVS (Concurrent Version System) or Subversion to maintain history of changes. It logs in to each device in the router table and saves the information by running various commands. The output is then mailed to a mail list, if any differences occur in the output. It includes backup tool and Audit tool.

- Track changes in the equipment configuration
- Track changes in the hardware (S/N, modules)
- Track version changes in the OS (IOS, CatOS versions)
- Recover from accidental configuration errors

Rancid currently supports Cisco routers, Juniper routers, Catalyst switches, Foundry switches, Redback NASs, ADC EZT3 muxes, MRTd, Alteon switches, and HP Procurve switches and a host of others[27]. It normally runs on UNIX/Linux platforms.

M. SNORT

Snort, a lightweight Network Intrusion Detection and Prevention System (NIDS/IPS)is designed to perform protocol analysis, content searching/matching, detect probes or attacks, OS fingerprinting attempts, Server Message Block (SMB) probes and much more[28]. It is capable of performing real-time traffic analysis and packet logging. These IDS watch packets on network using Sniffer mode. Packet logger mode logs the packets to the disk. Network intrusion detection mode analyzes network traffic. The raw packets are checked by the preprocessor and they are sent to detection engine, if certain type of behavior is found. From the detection engine, the packets are sent to Alerting/Logging components. If any sort of intruder activity is detected, Alerts are sent to the security administrator and it may be in the form of pop-up windows, e-mail, and logging to a console and so on. Alerts can also be stored in log files or databases like MYSQL and Postgres. For Linux and UNIX systems, snort requires Secure Shell (SSH) and Apache with Secure Socket Layer (SSL) and for Windows it requires IIS (Internet Information Servers [29].

N. NFDUMP/NFSEN

NFDUMP is basically implemented for capturing net flow data and processing them. This command line based, open source tool is written in C and it is very fast [30]. It stores the net flow data in time sliced files. It automatically rotates files every n minute. Analysing the data is basically done for a single file or by concatenating several files for a single run. NFDUMP has a powerful and fast filter engine. All flows are filtered before they are further processed. If no filter is given, any flow will be processed. It has four fixed output formats: raw, line, long and extended. Netflow Sensor (Nfsen) is a graphical web based front end for the NFDUMP Netflow tools. It is written in PHP and Perl. By using Round Robin Database it gives information about Netflow data like Flows, Packets and bytes and processes them within specified time span [31]. It gives the graphical overview over the Netflow data. It easily navigates through the Netflow data. Nfsen has both Web interface and Command line interface. The Backend plugins and Frontend plugins can be used to have different or additional needs to process and display Netflow data. Nfsen is a Open source tool under BSD License [32].

O. SmokePing

SmokePing, free Open source software, is used to show the latency of the connection to the server over a time interval and the packet loss. It can use pings, http requests, or SMTP requests to the server or network service to collect the latency information. Ping will quickly show whether a server is up and how fast it is responding. Test packets are sent out to the net and the amount taken by these packets to reach one place to another is measured. From this information the network health can be obtained. Round robin Database (RRD) is used to maintain all the data and the graphs can be drawn to give the minute information of each network connection [33]. All the characteristics of the ping packet responses can be expressed by using a single graph. SmokePing probe can be run remotely by Master/Slave concept. The master and slave communicate with each other via normal SmokePing web interface. SmokePing includes built-in probes for Cisco devices, Telnet, LDAP and many other protocols. It has highly configurable alerting system.

P. Munin

Munin (which means "memory")[34] is a network/system monitoring tool that analyses the performance of computers, networks, SANs, applications, weather measurements and much more. The information is presented in the form of graph through a web interface. It is implemented as master/node architecture where the master is connected to all the nodes at regular intervals and asks the nodes for data. Munin will then use the data to generate the corresponding graphs [35]. Every five minutes, it connects to all the servers it has to monitor, fetches the data and writes the data in hundreds of RRD (Round-Robin database) files. It then recreates all the HTML files and hundreds of PNG files. The Munin master is responsible for gathering data from Munin nodes. Munin is written in Perl and plugins are easy to write [36].

Q. NetDisco:

NetDisco is an Open Source web-based network management tool. It is designed for moderate to large networks. The configuration information and connection data for network devices are retrieved and set by SNMP (Simple Network Management Protocol) [37]. With the help of NetDisco the switch port of an end-user system by IP or MAC address can be located. NetDisco uses router tables and MAC forwarding tables to locate nodes on physical ports and track them by their IP Addresses. It also finds nodes by vendor. Each node maintains the ports that it has visited and the IP addresses it has used. It is controllable through Web interface or Command Line Interface (CLI). It can be easily extended for new network devices. Data is collected into a SQL database using SNMP and presented with a web interface and CLI.

R. WhatsUp Gold

It is a monitoring solution that discovers IP based network devices, maps, monitors, and alerts. This windows based tool includes monitoring modules for Microsoft Exchange server and SQL server. WhatsUp polls the network to identify attached devices [38]. The graphical representation of the network is used for accessing the operating status of any devices in the network. The entire network configuration can be managed from one interface. Active, Passive and Performance are the three types of monitors that can be assigned to a device. If a device does not respond to ping or TCP requests, it cannot be discovered by WhatsUp. Once the device is discovered, WhatsUp Gold uses SNMP (Simple Network Management Protocol) or WMI (Windows Management Instrumentation) data from individual devices to determine its manufacturer and model, components (such as fans, CPUs, and ard disks), operating system, and specific services. It logs two types of data: changes in network status such as a device going down; and, polling statistics for each device. From this data WhatsUp Gold can create several reports and graphs (to show the status of the network in different ways). It uses Microsoft's Open Database Connectivity (ODBC) data source [39].

S. *ZABBIX*:

Zabbix, a very famous open-source monitoring application that is designed to monitor performance and availability of servers, WEB applications, databases, networking equipment and many more. It auto-discovers the servers the server and network devices and is able to monitor thousands of devices [40]. Zabbix agent can be added to monitor the target computers for CPU Utilization, memory Utilization, Network Utilization, log monitoring and many more and stores the data in the Relational Database. Zabbix can be used to verify the availability of standard servers like SMTP (Simple Mail Transfer Protocol) or HTTP (Hypertext Transfer Protocol). The data can be displayed in the form of graphs and maps. It has very flexible notification mechanism and web based interface. Zabbix supports for both polling and trapping mechanisms. It requires MySQL or Postgres or Oracle as backend database.

T. NAV

Network Administration Visualized is an advanced software suite to monitor large computer networks. It automatically discovers network topology, monitors network load and outages, and can send alerts on network events by e-mail and SMS, allowing for flexible configuration of alert profiles. NAV [41] is free software. NAV offers a message system that displays operational messages, a maintenance tool to put devices on maintenance for a planned time period and thus suppress alarms, a cisco syslog Analyser that structures and lets you search syslog messages from cisco devices, a general mechanism for authentication and authorization of NAV users. Support LDAP and active directory. Use the user administration tool to manage users and on a group level set the appropriate authorization level. NAV administrators can "sudo" to other users to see/adjust their setup. NAV cannot pinpoint all the errors in network, but discovers serious errors. NAV does not generate precise report on how to solve a problem but gives alerts or clear indication that needed to be corrected. NAV does not provide end-end traffic data [42].

U. NetXMS

NetXMS [43] is a multi-platform, reliable and powerful network management and monitoring system. It offers event management, performance monitoring, alerting, reporting and graphing for the entire IT infrastructure model. NetXMS support for multiple operating systems and database engines, distributed network monitoring, auto-discovery, and business impact analysis tools, amongst others. NetXMS discovers the network automatically. It has three tire architecture. The monitoring agent collects information and is sent to the monitoring server for processing and storage. Using this information it monitors the status of network devices and hosts, collects performance data from network devices and servers. For each new device found NetXMS server tries to gather additional information using SNMP (Simple Network Management Protocol) and NetXMS agent, and then adds it to

database. Notification is sent via e-mail or SMS to system administrator in case of problems. NetXMS gives the option to run a web-based interface or a management console.

V. ZENOSS:

ZENOSS Core is a powerful open source IT monitoring platform that monitors applications, system log, servers, storage, networking and virtualization to provide availability and performance statistics[44]. ZENOSS core effectively manage the configuration, health and performance of network through a single integrated software package. It helps in automatic detection of network resources and configuration. ZENOSS uses the Zope application servers and MySQL for data storage and is written Python. This is built to address the challenges of dynamic data centre giving server administrators the ability to deliver service assurance [45]. ZENOSS supports Nagios plug-in format. It has a high performance event handling system and an advanced notification system via e-mail and SNMP (Simple Network Management Protocol)

III. CONCLUSION

The need for Network monitoring tools are increasing rapidly as the network keeps growing. These tools ease the administrator's job, not only by monitoring the network but also by fixing the network problem on time. This paper provides a survey of few monitoring tools based on their features, performance, and security.

REFERENCES

[1] http://www.arubanetworks.com /
[2] http://uct.com.do/wp-content/uploads/2012/03/AIRWAVE-Comprehensive-Management-for-Mobile-Enterprise-Networks.pdf
[3] http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd802570d0.html
[4] http://www.7signal.com/products/
[5] http://www.azuresol.com/7signal.htm
[6] https://plus.google.com/102485389301283523071/posts
[7] http://www.bigsister.ch/
[8] http://en.wikipedia.org/wiki/Big_Sister_(software)
[9] http://www.cacti.net/
[10]http://en.wikipedia.org/wiki/Cacti_(software)
[11]https://cug.org/5-publications/proceedings_attendee_lists/CUG09CD/S09_Proceedings/pages/authors/11-15Wednesday/14A-Davis/davis-paper.pdf
[12] http://cricket.sourceforge.net/
[13] http://staff.science.uva.nl/~jblom/gigaport/tools/monitor_tools.html
[14] http://oss.oetiker.ch/mrtg/doc/mrtg.en.html
[15] http://sssg1.whoi.edu/sssg/network_tools.html
[16] http://oss.oetiker.ch/rrdtool/
[17] http://en.wikipedia.org/wiki/RRDtool
[18] http://www.sans.org/reading-room/whitepapers/logging/effective-logging-kiwi-syslog-utility-201?show=effective-logging-kiwi-syslog-utility-201&cat=logging
[19] http://www.kiwisyslog.com
[20] http://www.kiwicattools.com/downloads/syslog/KiwiSyslogWebAccess.pdf
[21] http://www.splunk.com/product
[22] http://en.wikipedia.org/wiki/Splunk
[23] http://www.nagios.org/
[24] http://web.archive.org/web/20060501150621/http://www.netsaint.org/changelog.php
[25] http://en.wikipedia.org/wiki/Nagios
[26] http://www.opennms.org/wiki/RANCID_RWS
[27] http://www.shrubbery.net/rancid/
[28] http://www.snort.org/
[29] http://www.seren.net/documentation/unix%20utilities/Snort.pdf
[30]http://sourceforge.net/projects/nfdump/
[31] http://sourceforge.net/projects/nfsen/
[32]https://nsrc.org/workshops/2012/apnic34-nmm/raw-attachment/wiki/WikiStart/nfsen.pdf
[33]oss.oetiker.ch/Smokeping/doc/reading.en.html
[34] http://munin-monitoring.org/wiki/WikiStart
[35] http://en.wikipedia.org/wiki/Munin_(network_monitoring_application)
[36] https://wiki.archlinux.org/index.php/Munin
[37] http://www.netdisco.org/readme.html
[38] www.whatsupprofessional.com
[39] www.whatsupgold.com
[40]https://www.zabbix.org/
[41]http://www.linuxhomenetworking.com/
[42] https://nav.uninett.no/
[43] http://www.netxms.org/documentation/netxms-admin.pdf
[44] http://www.zenoss.com/
[45] http://sourceforge.net/projects/zenoss/